ABSTRACT

A server-assisted computational method for computing the RSA cryptography is delineated in this document. The method enables public-key functions on the resource-constrained devices, such as a mobile phone or a PDA, by leveraging the rich computing resources provided by the server-grade computers on the network. Public-key processing, which is computationally intensive as commonly known, if loaded solely on the constrained device, would easily overwhelm the processor capacity and electrical power supply. The server-assisted method enables such device to drive a powerful server computer on the Internet to carry out the public-key number-crunching job for its sake. Some near-completion results are communicated back to the device. From that, the final public-key cryptograph is derived. Privacy and security are the utmost important considerations in public-key systems. The present invention ensures the privacy of the device by blinding the server of the secret message and the crypto keys of the device. The merit is that the client device is able to accomplish the public-key processing with the help of the server, but without compromising the private crypto keys and confidential message code to the server.